

COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT FOR SUFFOLK COUNTY

SUFFOLK, ss.

No. SJ-2018-458

BOSTON GLOBE MEDIA PARTNERS, LLC,
Petitioner

v.

CHIEF JUSTICE OF THE TRIAL COURT and
CHIEF JUSTICE OF THE DISTRICT COURT DEPARTMENT,
Respondents

**RESPONDENTS' MEMORANDUM IN OPPOSITION TO PETITION FOR
DECLARATORY RELIEF¹ PURSUANT TO G.L. c. 211, § 3**

The petitioner, Boston Globe Media Partners, LLC, asserts that it has a presumptive right to access the records of any "show cause" hearing at which a judicial officer finds probable cause to believe that the accused committed a crime but declines to issue criminal charges against the accused (the "Records"). Contending that such a presumption of access is guaranteed by either the First Amendment of the United States Constitution, article 16 of the Massachusetts

¹ Although the petition is styled as one for "declaratory relief," the petitioner correctly observes (pet'n p. 2) that a declaratory judgment is not available against the judicial department. See G.L. c. 231A, § 2. Rather, the petitioner's claim implicates this Court's "general superintendence of the administration of all courts of inferior jurisdiction." G.L. c. 211, § 3 (2d paragraph). Thus this memorandum refers to the sought-after relief as "extraordinary" rather than "declaratory."

Declaration of Rights, or the common law of Massachusetts, the petitioner asks this Court for a corresponding award of extraordinary relief.

The respondents, the Chief Justice of the Trial Court and the Chief Justice of the District Court Department of the Trial Court, oppose the granting of such relief. First, the constitutional provisions that the petitioner invokes do not render the Records presumptively accessible, a conclusion that is compelled by Supreme Judicial Court precedent. See pp. 9-14 below. Second, Massachusetts common law does not render the Records presumptively accessible. See pp. 14-18 below. Third, Massachusetts common law does permit records of a particular show cause hearing to be made accessible on a case-specific basis--a principle that may entitle the petitioner to seek reconsideration in the Dorchester Division of the Boston Municipal Court ("Dorchester BMC") of whether to open the records of one particular show cause hearing that the petitioner has identified. See pp. 19-23 below.

BACKGROUND

The Role of Show Cause Hearings In the Justice Process

A "show cause" hearing is a proceeding at which a district court or . . . a justice, associate justice or special justice thereof, or . . . a clerk,

assistant clerk, temporary clerk or temporary assistant clerk thereof,"² determines whether to issue criminal process,³ and thus initiate a criminal prosecution, against a person accused of a crime or crimes. See generally G.L. c. 218, § 35A.

The process that leads to a show cause hearing begins when a complainant files, with the district court, an application for issuance of a criminal complaint against a person who is not under arrest.⁴ See generally G.L. c. 218, §§ 32, 35. If the accused presents an imminent threat of bodily injury, commission of a crime, or flight, the judicial officer may issue a complaint without convening a show cause hearing. G.L. c. 218, § 35A. But, if the accused does not present any such threat, the judicial

² The statute defines "district court" to also include the Boston Municipal Court and the Juvenile Court. See G.L. c. 218, § 35A. This memorandum similarly uses the term "district court" to include those two other courts, except where otherwise noted.

³ In the context of this petition, "criminal process" refers to a complaint charging the accused with a crime and the related summons or arrest warrant intended to procure her or his appearance in court. See generally G.L. c. 218, §§ 32-33.

⁴ Unlike many other states, Massachusetts permits anybody with knowledge of facts constituting an offense--not just a police officer--to file such an application. E.B. Cypher, 30 Mass. Prac., Criminal Practice & Procedure § 13:15 (4th ed. 2014); Mass. R. Crim. P. 3(g)(1); see also Bradford v. Knights, 427 Mass. 748, 751 (1998) (private citizen's right to seek criminal complaint is "something of an anomaly").

officer: (1) may convene a show cause hearing "in the case of a complaint for a felony which is not received from a law enforcement officer"; and (2) must convene a show cause hearing "in the case of a complaint for a misdemeanor or a complaint for a felony received from a law enforcement officer who so requests." G.L. c. 218, § 35A.

At the show cause hearing, the accused receives an "opportunity to be heard personally or by counsel in opposition to the issuance of any process based on such complaint." G.L. c. 218, § 35A. Thus the hearing "is held for the protection and benefit of the [accused], not for the benefit of the complainant." Victory Distributors, Inc. v. Ayer Div. of Dist. Court Dep't, 435 Mass. 136, 141-42 (2001).

The "legal function" of the hearing is "to determine whether there is probable cause to issue criminal process against the accused," without which no complaint may issue. Eagle-Tribune Publ'g Co. v. Clerk-Magistrate, 448 Mass. 647, 650 (2007); Mass. R. Crim. P. 3(g)(2); see G.L. c. 218, § 35A (judicial officer "may upon consideration of the evidence, obtained by hearing or otherwise, cause process to be issued unless there is no probable cause to believe that the person . . . has committed the offense charged"). But the hearing also has an "implicit purpose" to:

enable the [clerk-magistrate]⁵ to screen a variety of minor criminal or potentially criminal matters out of the criminal justice system through a combination of counseling, discussion, or threat of prosecution-- techniques which might be described as characteristic, in a general way, of the process of mediation. Thus, a show cause hearing . . . will often be used by a clerk-magistrate in an effort to bring about an informal settlement of grievances, typically relating to minor matters involving the frictions and altercations of daily life.

Eagle-Tribune, 448 Mass. at 650 (internal citations omitted; first alteration in original); accord Bradford, 427 Mass. at 751 ("[C]lerks and magistrates often use [show cause hearings] as an occasion to effect an informal settlement of grievances . . .").

In harmony with this "implicit purpose" of informal dispute resolution, a finding of probable cause to believe that the accused has committed an offense does not compel the judicial officer to issue a complaint. See G.L. c. 218, § 35A (judicial officer "may" cause process to be issued). Rather, in that situation, the Legislature has vested the judicial officer with discretion to choose whether to issue a complaint. This discretion is "ancillary to the discretion of prosecuting authorities to decide

⁵ Any judicial officer enumerated in section 35A may convene and conduct a show cause hearing. But, in practice, the hearing typically is held in the first instance before the clerk-magistrate, or an assistant clerk-magistrate, of the relevant district court.

whether to prosecute a particular case"; if a District Attorney or the Attorney General chooses to prosecute a charge, the judicial officer may not decline to issue a complaint that is supported by probable cause. Victory Distributors, 435 Mass. at 143.

Disposition of the Records of a Show Cause Hearing

If the show cause hearing results in issuance of a complaint, the judicial officer will then work with the complainant to prepare and sign the complaint, and will compel the accused's appearance in court through either a summons or an arrest warrant. G.L. c. 276, § 22. Once signed, the complaint is filed in court, the application for the complaint and other records relating to the show cause hearing become part of the court file, and the prosecution commences. See, e.g., G.L. c. 263, § 4 ("No person shall be held to answer in any court for an alleged crime, except upon an indictment by a grand jury or upon a complaint before a district court") (emphasis added); Commonwealth v. Vitale, 44 Mass. App. Ct. 908, 909 (1997) ("'[A] criminal proceeding shall be commenced in the District Court by a complaint,' not an application for a complaint.") (quoting Mass. R. Crim. P. 3; emphasis in Vitale).

If, however, the show cause hearing does not result in issuance of a complaint--including where the judicial officer finds probable cause but declines to

issue the complaint in her or his discretion--the clerk of the district court must note that denial on the face of the application, "maintain[] [the application] separately from other records of such court," and "destroy such application one year after the date [it] was filed" unless ordered otherwise by a judge.⁶ G.L. c. 218, § 35; see also E.B. Cypher, 30 Mass. Prac., Criminal Practice & Procedure § 13:27 (4th ed. 2014). Where the judicial officer who declines to issue the complaint is a clerk-magistrate (or an assistant, temporary, or temporary assistant clerk-magistrate), the complainant may seek rehearing of the application before a judge of the district court, who may likewise decline to issue the complaint despite the presence of probable cause. Bradford, 427 Mass. at 752-53.

The Petitioner's Factual Allegations

The petitioner alleges that, during the past year, it made two blanket requests to the judiciary for all "cases where probable cause was found, but no complaint was issued." Pet'n ¶¶ 23(a), 23(c), Exh. B, Exh. D. It alleges that both requests were denied. Id. ¶¶ 23(b), 23(d), Exh. C, Exh. E. The petitioner

⁶ These recordkeeping provisions do not apply to certain non-criminal applications made pursuant to the motor vehicle statutes. See G.L. c. 218, § 35 (citing G.L. c. 90, § 20C).

also alleges that, on August 3, 2018, it asked the Dorchester BMC for access to the records of a particular show cause hearing that resulted in a finding of probable cause but not in the issuance of a criminal complaint. Id. ¶ 23(e) & Exh. F. The petitioner alleges that, in response to this request, it “was advised that it was the Clerk-Magistrate’s policy not to provide access to show-cause hearings records unless criminal charges issue (regardless of whether probable cause was found or the other circumstances of the case).” Id. ¶ 23(e).

ARGUMENT

This Court should decline to award extraordinary relief. First, the constitutional provisions that the petitioner invokes do not render the Records presumptively accessible, a conclusion that is compelled by Supreme Judicial Court precedent. See pp. 9-14 below. Second, Massachusetts common law does not render the Records presumptively accessible. See pp. 14-18 below. Third, the common law does permit records of a particular show cause hearing to be made accessible on a case-specific basis--a principle that may entitle the petitioner to ask the Dorchester BMC to reconsider whether to open the records of the one particular show cause hearing that the petitioner has identified. See pp. 19-23 below.

I. THE CONSTITUTIONAL PROVISIONS THAT THE PETITIONER INVOKES DO NOT RENDER THE RECORDS PRESUMPTIVELY ACCESSIBLE.

The petitioner argues that presumptive access to the Records is guaranteed either by the First Amendment of the Federal Constitution or by article 16 of the Massachusetts Declaration of Rights. But the SJC has previously concluded that neither the First Amendment (see pp. 9-12 below) nor article 16 (see pp. 12-14 below) supports such a presumption.

A. The SJC Has Previously Concluded that the Records Are Not Presumptively Accessible Under the First Amendment.

The petitioner argues (memo. pp. 28-30) that the Records are presumptively accessible under the First Amendment. This argument is unavailing because, as the SJC has previously concluded, show cause hearings satisfy neither of the considerations required to make out a presumption of access under the First Amendment.

The First Amendment guarantees access to criminal court proceedings where two considerations are met. Press-Enterprise Co. v. Superior Court, 478 U.S. 1, 8 (1986). The first is "whether the place and process have historically been open to the press and general public." Id. The second is "whether public access plays a significant positive role in the functioning of the particular process in question." Id.

The SJC has previously applied these two considerations to conclude that the First Amendment

does not render show cause hearings presumptively accessible. See Eagle-Tribune, 448 Mass. at 651-56. With respect to historical experience, the SJC found that, from their inception as "informal opportunities for the accused to be heard on the question whether to issue criminal process, show cause hearings have always been [p]resumptively . . . private and as informal as circumstances will permit." Id. at 652 (alternations in original; citations omitted). With respect to the role of access in show cause hearings' functioning, the SJC found that, because the hearings are held "for the protection and benefit of the accused, and allow[] the clerk-magistrate to screen out baseless complaints with minimal harm to the accused's reputation," public access would frustrate, rather than enhance, the hearings' effectiveness. Id. at 656 ("[T]he ability of clerk-magistrates to resolve commonplace disputes without the need for criminal prosecution could be compromised by hearings open to the public, which may inflame the animosities involved.").

In reaching this conclusion, the SJC compared pre-complaint show cause hearings to pre-indictment grand jury proceedings; id. at 655; the grand jury being a "classic example" of a proceeding that "would be totally frustrated if conducted openly." Press-Enterprise, 478 U.S. at 8-9; accord Globe Newspaper

Co. v. Commonwealth, 407 Mass. 879, 887 (1990) ("There are numerous litigation-related events to which the public does not have a constitutional or any other right of access. They include grand jury proceedings . . . and lobby conferences").

The SJC's conclusions--which apply to all show cause hearings--carry the same force in the specific circumstance where a judicial officer finds probable cause to issue a complaint, but declines in the interests of justice to institute criminal proceedings by issuing a complaint. As the SJC recognized, show cause hearings are traditionally private and informal, characteristics that do not vary based on the presence of probable cause in a particular application. Eagle-Tribune, 448 Mass. at 655-56 ("[T]o the extent that show cause hearings often function as informal dispute resolution sessions akin to court-facilitated mediation, they share in a tradition not of openness, but of privacy."). Similarly, a show cause hearing's utility as a forum for informal dispute resolution depends on the willingness of the complainant and the accused to engage in candid and constructive conversation at that hearing, not on the presence of probable cause. Id. Thus, to conclude that all applications featuring probable cause are presumptively accessible for public inspection would have a chilling effect on the complainant and the

accused, and thus impair the hearings' "implicit function" of informal resolution.

The petitioner argues (memo. pp. 2-3) that Eagle-Tribune addressed only the right to attend a live show cause hearing, not the right to peruse the records of a concluded hearing. But the difference between those two modes of access is not material to the First Amendment analysis. See Press-Enterprise, 478 U.S. at 13; accord Commonwealth v. Winfield, 464 Mass. 672, 675 (2013) (noting that Press-Enterprise "equated the right of access to attend [a] hearing with the right to obtain a transcript of the hearing"). Thus, where the First Amendment grants no right to attend a particular proceeding, it grants no right to obtain the records of that proceeding. See Globe Newspaper Co. v. Pokaski, 868 F.2d 497, 509 (1st Cir. 1989).

B. The SJC Has Previously Concluded that the Records Are Not Presumptively Accessible Under Article 16.

The petitioner also argues (memo. pp. 30-32) that the Records are presumptively accessible under article 16 of the Massachusetts Declaration of Rights. The petitioner asserts (memo. p. 30) that, "[a]lthough the precise issue raised here never has been considered by the Supreme Judicial Court, the provisions of [a]rticle 16 have been held to extend protections even greater than those of the First Amendment."

But, although article 16 has sometimes been interpreted more broadly than the First Amendment in contexts bearing no resemblance to this petition,⁷ the SJC has indeed considered and rejected the precise issue raised by the petitioner here. Specifically, in Eagle-Tribune, the SJC observed that "the criteria which have been established by the United States Supreme Court for judging claims arising under the First Amendment [concerning accessibility of criminal court proceedings] . . . are equally appropriate to claims brought under cognate provisions of the Massachusetts Constitution." 448 Mass. at 651 n.10, quoting Opinions of the Justices to the House of Representatives, 387 Mass. 1201, 1202 (1982). The petitioner offers no reason to disregard Eagle-Tribune's teaching that article 16 provides no greater

⁷ See, e.g., Commonwealth v. Sees, 374 Mass. 532 (1978) (art. 16 prohibits bar manager who permitted semi-nude dance performance from being convicted for violating local ordinance prohibiting such things) (cited in petitioner's brief); Cabaret Enterprises v. Alcoholic Beverages Control Commission, 393 Mass. 13 (1984) (art. 16 prohibits revocation of liquor license based on bar's permitting nude dancing on premises) (cited in petitioner's brief); Lyons v. Globe Newspaper Co., 415 Mass. 258 (1993) (citing art. 16 and First Amendment as alternative bases to affirm dismissal of defamation claim arising out of publication of article about protestors at political gathering) (cited in petitioner's brief).

access to records of show cause hearings than does the First Amendment.

II. MASSACHUSETTS COMMON LAW DOES NOT RENDER THE RECORDS PRESUMPTIVELY ACCESSIBLE.

The petitioner argues (memo. pp. 17-23) that the Records are presumptively accessible under Massachusetts common law, but this argument fails for at least two reasons. First, the common law presumption of access does not extend to papers of the Records' type. See pp. 14-17 below. Second, the Legislature has required that the Records be treated differently from ordinary court papers, a requirement that is inconsistent with a common law presumption of access. See pp. 17-18 below.

A. The Common Law Presumption of Access Does Not Extend To Papers of The Records' Type.

The common law presumes that most papers held by a court are to be accessible to the public, a concept sometimes described as a "general principle of publicity." E.g., Commonwealth v. Blondin, 324 Mass. 564, 571 (1949); Winfield, 464 Mass. at 678. But that presumption does not extend to every paper held by a court. Winfield, 464 Mass. at 679. Specifically, although a paper kept in the court's file on a given case is presumed to be accessible, a paper that belongs to the court but is not kept in the court's case file is presumed to be accessible only if it is

"so important to public understanding of the judicial proceeding that it should be presumed to be public, so that the public may 'assume a significant, positive role in the functioning of the judicial system.'" Id. at 680-81.

Here, the Records are not kept in the court's file on a given case; to the contrary, because the underlying show cause hearing did not result in issuance of a criminal complaint, the Records are "maintained separately from other records of [the] court" and are destroyed after only one year. G.L. c. 218, § 35.

Thus, the Records' amenability to a presumption of access depends on whether public access plays a significant, positive role in the functioning of show cause hearings. As discussed above (pp. 9-10), the SJC has previously concluded, under the rubric of the First Amendment, that public access does not play such a role in show cause hearings. See Eagle-Tribune, 448 Mass. at 656. That conclusion is equally valid under the rubric of the common law. And the similarity between show cause hearings and grand jury proceedings further supports the conclusion that the Records are not amenable to a presumption of access under the

common law.⁸ See, e.g., In re Motions of Dow Jones & Co., 142 F.3d 496, 504 (D.C. Cir. 1998) (no common law right of access to grand jury materials); In re Gwinnett Cty. Grand Jury, 284 Ga. 510, 513-14 (2008) (same); Daily Journal Corp. v. Superior Court, 20 Cal. 4th 1117, 1132 (1999) (same); United States v. Smith, 123 F.3d 140, 155-56 (3d Cir. 1997) (same; "[u]nlike judicial records to which a presumption of access attaches when filed with a court, grand jury materials have historically been inaccessible to the press and the general public, and are therefore not judicial records in the same sense").

The petitioner argues (memo. pp. 19-20) that a judicial officer's finding of probable cause to support issuance of a complaint at a show cause hearing is analogous to a finding of probable cause to support issuance of an arrest warrant or a search warrant. The petitioner suggests that, in those contexts, the probable cause finding "triggers the public's common law right of access." Under controlling law, however, a right of access is not

⁸ The petitioner may argue that a grand jury is different because its membership is not limited to one appointed clerk-magistrate. But a complainant's ability to obtain rehearing, by a district court judge, of a clerk's denial of an application diminishes the risk that a meritorious application fails to result in issuance of criminal charges due to the clerk.

triggered by a finding of probable cause to issue a warrant, but rather by the filing of the relevant papers with the court once the warrant has been returned. See, e.g., Commonwealth v. George W. Prescott Publ'g Co., 463 Mass. 258, 260 (2012) (search warrant materials become presumptively accessible "when filed in court . . . once the warrant has been returned"); Republican Co. v. Appeals Court, 442 Mass. 218, 222-23 (2004) ("[U]nder the common law . . . the public has a presumptive right of access to affidavits filed in support of search warrant applications once the warrant is returned."). The fact that the Records are never filed in court refutes any comparison with warrant application papers.

B. The Legislature Has Required That The Records Be Treated Differently from Ordinary Court Papers.

Coexisting with the presumption that most papers held by a court are to accessible to the public "are statutes which, for a variety of reasons that can be surmised, limit or authorize limitation of access to court proceedings and official records." Ottaway Newspapers, Inc. v. Appeals Court, 372 Mass. 539, 546 (1977). "Unless there is a violation of a constitutional guaranty, the Legislature may modify or abrogate common law practices" relating to public access to court papers. New Bedford Standard-Times

Publ'g Co. v. Clerk, 377 Mass. 404, 410 (1979); accord
In re Globe Newspaper Co., Inc., 461 Mass. 113, 116-18
(2011) (enactment of statute concerning impoundment of
inquest report partially abrogates common law
principles, established by earlier SJC decision, on
same subject); Ottaway Newspapers, 372 Mass. at 547-49
(statute limiting disclosure of records concerning
administrative proceedings to remove bank director
supports impoundment of those records when filed in
court); Boston Herald, Inc. v. Sharpe, 432 Mass. 593,
607-08 (2000) (where statute limits disclosure of
identified portions of court file on domestic violence
restraining order, presumption of public access
applies only to portions of court file not identified
by statute).

Here, the Legislature has specifically required
that the records of a show cause hearing that does not
result in issuance of a criminal complaint be
"maintained separately from other records of [the]
court" and "destroy[ed] . . . one year after the date
[it] was filed" unless ordered otherwise by a judge.
G.L. c. 218, § 35. The Legislature thus has
demonstrated its intent that the Records not be
treated as ordinary court papers presumptively
accessible under the common law. For this additional
reason, the Records are not amenable to a presumption
of access under the common law.

**III. THE COMMON LAW PERMITS RECORDS OF A PARTICULAR
SHOW CAUSE HEARING TO BE MADE ACCESSIBLE ON A
CASE-SPECIFIC BASIS.**

That the Records are not presumptively accessible does not mean that they are always inaccessible. Winfield, 464 Mass. at 681. Rather, it means that a person seeking to access such records in a particular case bears the burden of demonstrating that access is consistent with the interests of justice in the circumstances of that case. See id. at 681.

This case-specific approach is consistent with District Court practice standards.⁹ Specifically, those standards permit access to records where the person seeking them shows that "legitimate public interests outweigh the accused's right of privacy" in view of the individual circumstances of the case.¹⁰ See District Court Standards of Judicial Practice: The Complaint Procedure §§ 3:15, 5:02 (2008); cf. In re Application for Criminal Complaint, 477 Mass. 1010, 1011 (2017) (affirming Single Justice's rejection of

⁹ The District Court Standards of Judicial Practice are "administrative regulations" that, although not binding in the same sense as statutory or decisional law, represent "statements of desirable practice" and form "a field guide or practice manual for clerk-magistrates." Commonwealth v. Clerk-Magistrate, 439 Mass. 352, 357 (2003).

¹⁰ Relief from a clerk-magistrate's denial of a request for access may be sought in extraordinary cases from a single justice of this Court. Eagle-Tribune, 448 Mass. at 657.

proposed categorical rule that application must be transferred to different district court where accused is police officer; "existing procedural safeguards, including rehearing by a judge, are adequate to ensure fair consideration"). Further, the Chief Justice of the Trial Court recently convened a Trial Court Working Group to consider a variety of issues relating to show cause hearings, including whether the District Court standards should be amended as they relate to access to the hearings and related records, as well as the adoption of standards by the Boston Municipal Court. That group has just begun its work, and it is too early to suggest what changes if any it might propose. But the group's membership includes current and former judges and clerk-magistrates from the District Court and the Boston Municipal Court, who are very familiar with the day-to-day realities of show cause hearings; the Chief Justice looks forward to receiving their considered views on these issues.

The case-specific approach also is consistent with the petitioner's suggestion (memo. pp. 27-28) that issues of access "are best addressed on a case-by-case basis" Although the petitioner prefers (memo. pp. 24-28) "case-by-case" consideration to take the form of impoundment orders interposed against a baseline presumption of access (which presumption is inappropriate for reasons discussed at

pages 14-18 above), the petitioner's insight is a valid one: The sheer range of circumstances that might be reflected in a show cause hearing suggests that issues of access should not turn on a "one-size-fits-all" presumption.

And this case-specific approach is consistent with the fact that many criminal complaint applications feature allegations of "more minor matters [that] may include the frictions and altercations of daily life, which may not attract the attention of the police or the public prosecutor but yet may rankle enough that resolution is required if peace is to be maintained." Bradford, 427 Mass. at 751. In reality, some of these allegations will be more appropriate to publicize than others will.

Applying this case-specific approach here, the petitioner may be entitled to seek relief in the Dorchester BMC. Specifically, the petitioner alleges that, on August 3, 2018, it asked the Dorchester BMC for access to the records of a particular show cause hearing that resulted in a finding of probable cause but not in the issuance of a criminal complaint. Id. ¶ 23(e) & Exh. F. The petitioner alleges that, in response to this request, it "was advised that it was the Clerk-Magistrate's policy not to provide access to show-cause hearings records unless criminal charges issue (regardless of whether probable cause was found

or the other circumstances of the case).” Id. ¶ 23(e).

Under the District Court standards described above, the petitioner’s request would be evaluated as to whether granting access to the requested records would be consistent with the interests of justice.¹¹ Even though, as a division of the Boston Municipal Court, the Dorchester BMC is not subject to the District Court standards, the Dorchester BMC could have exercised its discretion to follow the District Court standards in response to the petitioner’s request. Cf. In re Application for Criminal Complaint, 477 Mass. at 1012 n.3 (in case arising out of Boston Municipal Court, suggesting that “[t]he public might be better served if the BMC would formalize its practice in written standards,” and favorably citing District Court standards). In alleging (pet’n ¶ 23(e)) that its request was denied on the basis of a blanket policy of the Dorchester BMC, the petitioner seems to suggest a contravention

¹¹ This, of course, assumes that the records still existed at the time of the petitioner’s request. The petitioner alleges that the sought-after application underlying the show cause hearing was filed on January 4, 2017, and that the show cause hearing occurred on June 30, 2017. Pet’n Exh. F. If those allegations are true, the relevant records might have been subject to destruction as early as January 4, 2018--some seven months before the petitioner requested them. See generally G.L. c. 218, § 35.

of the principles expressed in the District Court standards. Thus, the petitioner might be entitled to seek reconsideration in the Dorchester BMC, and to challenge any further denial of relief in that particular case before the single justice of this Court, pursuant to the procedure described in Eagle-Tribune. See 448 Mass. at 657.

CONCLUSION

For all of the foregoing reasons, the Chief Justice of the Trial Court and the Chief Justice of the District Court Department of the Trial Court respectfully request that the Court deny the petitioner's request for extraordinary relief.

Respectfully submitted,

MAURA HEALEY
ATTORNEY GENERAL



December 7, 2018

Eric A. Haskell, BBO No. 665533
Assistant Attorney General
One Ashburton Place
Boston, Massachusetts 02108
617-963-2855
eric.haskell@state.ma.us

CERTIFICATE OF SERVICE

I certify that a true copy of the foregoing "Memorandum in Opposition" was transmitted to the petitioner's counsel of record via U.S. Mail and e-mail as follows:

Jonathan M. Albano, Esq.
Morgan, Lewis & Bockius LLP
One Federal Street
Boston, Mass. 02110
jonathan.albano@morganlewis.com

December 7, 2018

A handwritten signature in black ink, appearing to read "Eric A. Haskell", written over a horizontal line.

Eric A. Haskell
Assistant Attorney General

COMMONWEALTH OF MASSACHUSETTS

The Appeals Court

SUFFOLK, SS.

No. 2018-P-0401

BOSTON GLOBE MEDIA PARTNERS, LLC,
Plaintiff-Appellee,

v.

DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES, MASSACHUSETTS
STATE POLICE, BOSTON POLICE DEPARTMENT,
Defendants-Appellants.

ON APPEAL FROM A JUDGMENT OF THE SUPERIOR COURT

REPLY BRIEF OF THE STATE APPELLANTS

MAURA HEALEY

Attorney General

Elizabeth N. Dewar, BBO No. 680722

State Solicitor

Daniel J. Hammond, BBO No. 559475

Assistant Attorney General

One Ashburton Place

Boston, Massachusetts 02108

(617) 963-2204

bessie.dewar@mass.gov

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	3
ARGUMENT.....	6
I. DCJIS’s Interpretation of the Statutory CORI Definition as Including Booking Photographs and Arrest- and Charge- Related Police Reports Should Be Upheld.....	6
A. DCJIS’s interpretation of the statute’s text is reasonable and faithful to the Legislature’s manifest concern for protecting the information of arrestees.....	7
B. The statute and DCJIS’s regulations provide a remedy insofar as law enforcement agencies improperly release CORI, including booking photographs or police reports.....	15
II. The CORI Law’s Text and Its Recognized Purposes Refute the Globe’s Contention That the 2010 Amendments Eliminated All CORI Protections Except for the Contents of DCJIS’s Database.....	18
III. Booking Photographs and Police Reports Do Not Categorically Fall Within the CORI Exceptions Making Public Certain Otherwise-Protected Records.....	22
CONCLUSION.....	25
ADDENDUM.....	28

TABLE OF AUTHORITIES

Cases

<i>Bellin v. Kelley</i> , 435 Mass. 261 (2001).....	7, 16
<i>Biogen IDEC MA, Inc. v. Treasurer</i> , 454 Mass. 174 (2009).....	9-11
<i>Borden v. Comm’r of Pub. Health</i> , 388 Mass. 707 (1983).....	6, 14
<i>Commonwealth v. Pon</i> , 469 Mass. 296 (2014).....	20-22
<i>Globe Newspaper Co. v. Dist. Att’y for the Middle Dist.</i> , 439 Mass. 374 (2003).....	23-24
<i>Globe Newspaper Co. v. Fenton</i> , 819 F. Supp. 89 (D. Mass. 1993).....	19
<i>Greater Boston Real Estate Bd. v. Dep’t of Tel. & Energy</i> , 438 Mass. 197 (2002).....	9
<i>Purity Supreme, Inc. v. Att’y Gen.</i> , 38 Mass. 762 (1980).....	6
<i>Royal Indem. Co. v. Blakely</i> , 372 Mass. 86 (1977).....	24
<i>Souza v. Registrar of Motor Vehicles</i> , 462 Mass. 227 (2012).....	12
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968).....	8

Constitutional Provisions and Statutes

U.S. Const., amend. 1.....	19
G.L. c. 4, § 7, cl. 26(a).....	14, 25
G.L. c. 6, § 167.....	<i>passim</i>
G.L. c. 6, § 167A(c).....	19
G.L. c. 6, § 171.....	13, 19
G.L. c. 6, § 171A.....	19

G.L. c. 6, § 172.....	<i>passim</i>
§ 172(f).....	22
§ 172(m).....	11-12, 19, 23-25
§ 172(m)(1).....	23-25
§ 172(m)(2).....	22-24
G.L. c. 6, § 172B.....	11
G.L. c. 6, § 172D.....	11
G.L. c. 6, § 172F.....	11
G.L. c. 6, § 175.....	19
G.L. c. 6, § 178.....	15-16, 22, 26
G.L. c. 6, § 178B.....	19
G.L. c. 41, § 98F.....	24-25
G.L. c. 276, § 100E <i>et seq.</i>	19-20
§ 100H.....	20
§ 100L(a).....	20
St. 1972, c. 805, § 1.....	12

Regulations

803 CMR 2.00 <i>et seq.</i>	12
803 CMR 2.01(4).....	13
803 CMR 2.02.....	13
803 CMR 2.03.....	6, 7, 9, 12-13
2.03(3).....	14
2.03(4).....	6-7, 9, 12-13
2.03(5)(b).....	13
2.03(5)(e).....	13
803 CMR 2.25.....	12, 16
803 CMR 2.26(3)(1).....	16
803 CMR 2.26(3)(m).....	16

803 CMR 7.10.....	15
803 CMR 7.12.....	16

ARGUMENT

I. DCJIS's Interpretation of the Statutory CORI Definition as Including Booking Photographs and Arrest- and Charge-Related Police Reports Should Be Upheld.

This Court should reject the Globe's contention that the CORI statute protects only information regarding criminal cases formally commenced in court, Br. 25, as opposed to, under DCJIS's regulation interpreting the statute, information starting at "the point when a criminal investigation is sufficiently complete that the investigating officer takes actions toward bringing a specific suspect to court." 803 CMR 2.03(4). The Globe does not dispute that DCJIS's interpretation of the CORI law - a law DCJIS is charged with administering - is entitled to "all the deference due to a statute." *Borden v. Comm'r of Public Health*, 388 Mass. 707, 723 (1983); see Globe Br. 28 (arguing only that the agency may not issue regulations in conflict with the statute). And the Globe has failed to meet its high burden of "prov[ing] 'the absence of any conceivable ground upon which [DCJIS's regulation] may be upheld.'" *Borden*, 388 Mass. at 722-23 (quoting *Purity Supreme, Inc. v. Att'y Gen.*, 38 Mass. 762, 776 (1980)). Because DCJIS's regulation reasonably interprets the CORI definition as a whole - including not only its opening broad sentence, but also the subsequent limiting sentences - DCJIS's interpretation should be upheld. See, e.g.,

Bellin v. Kelley, 435 Mass. 261, 265-69 (2001) (upholding as "reasonable" a regulation promulgated by DCJIS's predecessor agency).

A. DCJIS's interpretation of the statute's text is reasonable and faithful to the Legislature's manifest concern for protecting the information of arrestees.

As described more fully in the opening brief, DCJIS's regulations reasonably interpret the CORI law to protect information regarding identifiable individuals beginning at "the point when a criminal investigation is sufficiently complete that the investigating officer takes actions toward bringing a specific suspect to court," 803 CMR 2.03(4), and such protections therefore extend to booking photographs and arrest- and charge-related police reports. DCJIS's interpretation reconciles the statutory definition's various clauses: both (1) the opening sentence, protecting "arrest"- and "charge"-related "records and data in any communicable form" compiled by a "Massachusetts criminal justice agency," G.L. c. 6, § 167, and (2) the subsequent sentences refining the "CORI" definition in various respects, including regarding proceedings dismissed prior to arraignment, intelligence information, and, under the version of the statute in effect until April 13, 2018, information recorded prior to "the initiation of criminal proceedings." See Comm. Br. 20-32. DCJIS's

regulation also accords with many other aspects of the CORI law reflecting the Legislature's longstanding understanding that arrest-related information is protected. See *id.* at 23-25. The Globe fails in its various attempts to refute the reasonableness of this interpretation.

First, the Globe relies on dictionary definitions of the words "initiation" and "proceedings" to stitch together the conclusion that the Legislature's former limitation of CORI to information recorded as the result of "the initiation of criminal proceedings" necessarily referred only to information regarding matters actually adjudicated in court. Globe Br. 23-24. Such is one reasonable understanding of that phrase in isolation, but it is only one possible understanding,¹ and it is in strong tension with the statute; the CORI definition expressly protects information regarding "arrests" (which commonly occur prior to any *judicial* proceedings), G.L. c. 6, § 167, and many other aspects of the CORI law, discussed further below, indicate the Legislature's intention

¹ See Boston Police Dep't Br. 10-11 (collecting cases referring to arrest as the initiating event in a criminal proceeding, including, *e.g.*, *Terry v. Ohio*, 392 U.S. 1, 26 (1968) ("An arrest is the initial stage of a criminal prosecution."), as well as statutes evincing the significance of an arrest as an intrusion on a person's liberty that may entail further proceedings such as consideration of bail).

that arrest-related information be protected. By contrast, DCJIS's interpretation of the phrase as a whole - under which such proceedings are "initiated" once "the investigating officer takes actions toward bringing a specific suspect to court," 803 CMR 2.03(4) - better accords with the Legislature's evident intention to protect "arrest"-related information. DCJIS's interpretation is thus at least reasonable and should be upheld. *See Biogen IDEC MA, Inc. v. Treasurer*, 454 Mass. 174, 186 n.22 (2009) (noting that "[c]ourts frequently resort to dictionaries" but that "[e]xcessive reliance on the plain meaning rule . . . may improperly invade the policy-making province of an administrative agency," and "[s]urrounding statutory language, the statute's purpose, and its legislative history, if any, also may assist courts in determining whether the relevant statutory language may plausibly be interpreted in more than one way").²

² Accordingly, the Globe's citations to cases such as *Greater Boston Real Estate Board v. Department of Telecommunications & Energy*, 438 Mass. 197, 204 (2002), for the proposition that "regulations aimed at persons not within the class of persons that the Legislature authorized the department to regulate were *ultra vires* of the enabling legislation," Br. 30, are unavailing. The CORI law's protections by their express terms are aimed at the "arrest"-related information of any "identifiable individual," G.L. c. 6, § 167, albeit with a series of exceptions that DCJIS has duly acknowledged, interpreted, and implemented in its regulations, *see infra* at 10-14. And the Globe's broader argument that DCJIS's

(footnote continued)

Second, the Globe's view of the new limitation added on April 13, 2018, amending the definition of CORI to include only information "recorded in criminal proceedings that are not dismissed before arraignment," G.L. c. 6, § 167, is similarly in tension with the statute as a whole and indeed is untenable in light of the available legislative history. That history confirms DCJIS's own reasonable understanding: that this provision was added as part of the recent criminal justice reforms to provide *additional* privacy protection to persons whose cases are dismissed prior to arraignment, ensuring that this information is not subject to disclosure via the DCJIS database. See Comm. Br. 22. To read this language as the Globe proposes - as precluding any CORI protection whatsoever for matters that are never arraigned - is to suggest that, in the midst of a statutory amendment designed to protect the privacy of individuals' prior interactions with the criminal justice system, the Legislature paradoxically added a clause that would *reduce* the level of privacy afforded to individuals whose cases never even made it to court. The Globe

regulation is *ultra vires* under the Globe's reading of the statute, Br. 29-30, fails to grapple with the deference due to DCJIS's regulations, which must be upheld so long as they are a reasonable interpretation (even if not the only rational interpretation). See *Biogen IDEC*, 454 Mass. at 187.

offers no explanation as to why the Legislature would intend such a meaning, see Globe Br. 25-26 – nor is any rational explanation readily apparent.³

Third, the Globe fails in its partial attempt to explain away the numerous other aspects of the CORI law evincing the Legislature's intention to protect arrest-related information. With respect to a number of these statutory provisions, the Globe offers no response, not even mentioning them in its brief. See, e.g., Comm. Br. 23-24 (discussing G.L. c. 6, §§ 172B, 172D, 172F); Globe Br. 6 (no mention). And the Globe does not dispute that its own interpretation would render superfluous provisions in the CORI law making police departments' chronological booking logs public "[n]otwithstanding" the CORI law's protections for arrest-related information, G.L. c. 6, § 172(m) – provisions that would be unnecessary if all such information were unprotected anyway. See Comm. Br. 24-25. The Globe's only answer is to argue that

³ DCJIS and MSP acknowledge that the "dismissed before arraignment" provision – which bars information about such cases from inclusion in the database maintained by DCJIS – thus operates differently from the other CORI definition exceptions (such as for intelligence information), which categorically exclude certain information from CORI protection altogether. Cf. Globe Br. 37 n.6. However, DCJIS's interpretation gives effect to each of the statute's provisions, is reasonable in light of the statute as a whole, and furthers the Legislature's evident aims regarding each exception. See *Biogen IDEC*, 454 Mass. at 186 n.22.

§ 172(m) is an inoperative vestige of a past regime in which CORI protections did extend further. See *Globe Br. 39*. But this Court should read the statute to give effect to all of its provisions. See *Souza v. Registrar of Motor Vehicles*, 462 Mass. 227, 233 (2012). Moreover, the "initiation of criminal proceedings" limitation was part of the CORI definition from the law's inception and thus has always co-existed with § 172(m). See St. 1972, c. 805, § 1. DCJIS's interpretation reasonably harmonizes these longstanding provisions.⁴

⁴ There is no merit to the *Globe*'s further argument that DCJIS's interpretation of "initiation of criminal proceedings" applies only to iCORI and not to paper records because the regulation begins with the phrase "[f]or purposes of 803 CMR 2.00," 803 CMR 2.03(4) – purposes the *Globe* construes as relating solely to iCORI electronic records. *Globe Br. 30-32*. First, DCJIS's regulations interpret the statute, and it is the statute that establishes and ultimately governs CORI protections. See Comm. Br. 31 n.8. That statute expressly states that CORI is information "in any communicable form," G.L. c. 6, § 167, thus foreclosing a "no paper records" interpretation. Second, while DCJIS's regulations naturally heavily focus on the iCORI system and users thereof due to DCJIS's mandate to establish and administer the system as the means of regulated access to CORI, DCJIS's regulations – including 803 CMR 2.00 et seq. – have broader purposes applicable to CORI generally. See, e.g., 803 CMR 2.01(2) (providing that 803 CMR 2.00 "sets forth" not only "the establishment and use of the iCORI system" but also, e.g., "CORI complaint procedures" generally); 803 CMR 2.25 (prescribing complaint procedures for "any violation(s) of the CORI laws and regulations," including "improper access to, or dissemination of, CORI"). Moreover and in any case,

(footnote continued)

Fourth and finally, the Globe cannot prevail with its argument that arrest- and charge-related information is all unprotected "intelligence information" unless a judicial proceeding occurs. See Comm. Br. 32-36. DCJIS's regulations adopt the statutory definition of "intelligence information" and duly exclude such information from protection. See G.L. c. 6, § 167; 803 CMR 2.02, 2.03(5)(e). DCJIS's regulation interpreting the statutory CORI definition is consistent with the intelligence-information exception, because it draws a reasonable, practical dividing line between unprotected intelligence information and protected CORI: information is protected starting at the "the point when a criminal investigation is sufficiently complete that the investigating officer takes actions toward bringing a specific suspect to court." 803 CMR 2.03(4); *see also* 803 CMR 2.03(5)(b) (excluding from CORI protection "photographs, fingerprints, or other identifying data of an individual used for investigative purposes, provided the individual is not identified"). Booking photographs, created upon an arrest, plainly fall within this definition, as do arrest- and charge-

803 CMR 2.01(4) expressly states that nothing in the regulations "shall be interpreted to limit the authority granted to the Criminal Record Review Board (CRRB) or to [DCJIS] by the Massachusetts General Laws." That authority includes broad powers to regulate CORI generally. See, e.g., G.L. c. 6, § 171.

related police reports relating to a specific identifiable individual. See 803 CMR 2.03(3) (providing that CORI shall include, *inter alia*, "photographs . . . recorded as the result of the initiation of a criminal proceeding"). To be sure, as the Globe points out, Br. 44-45, the intelligence information exception does serve a purpose in limiting the scope of "CORI"; among other reasons, if information relates to early parts of an investigation, it is hardly accurate evidence of a criminal record. However, information regarding an "arrest" or "charge" is protected. G.L. c. 6, § 167.

In sum, the Globe has not established that there is no "conceivable ground upon which [DCJIS's regulations] may be upheld." *Borden*, 388 Mass. at 722-23 (quotation omitted). To the contrary, DCJIS's regulations interpreting the statute to protect both booking photographs and arrest- and charge-related police reports are reasonable and should be upheld. As a result, the disputed records are protected as CORI and exempt from disclosure under the Public Records Law as records that are "specifically or by necessary implication exempted from disclosure by statute." G.L. c. 4, § 7, cl. 26(a).

B. The statute and DCJIS's regulations provide a remedy insofar as law enforcement agencies improperly release CORI, including booking photographs or police reports.

The Globe's brief repeatedly mentions that law enforcement agencies sometimes release booking photographs and arrest-related police reports. See, e.g., Globe Br. 10-12, 42 nn.8-9. Given that agencies are authorized to share CORI for various reasons in carrying out their official duties, the fact of such releases is not inconsistent with CORI protection for booking photographs and arrest- and charge-related reports. And, if agencies violate the CORI law, the statute and regulations provide remedies.

As part of DCJIS's broad authority to regulate access to CORI, DCJIS regulates the circumstances in which criminal justice agencies may release CORI. See 803 CMR 7.10. These regulations provide that criminal justice agencies may, for example, share CORI with other criminal justice agencies "for official criminal justice purposes"; may disseminate CORI when the CORI is "specifically related to, and contemporaneous with, an investigation or prosecution"; may disclose certain CORI with school leadership regarding students aged 17 or older; and may disclose CORI "as otherwise authorized by law in the interest of public safety." 803 CMR 7.10(1)-(6) (Add. 33); see also G.L. c. 6, § 178 (CORI penalty provisions "shall not apply to . . . a law enforcement officer who, in good faith,

obtains or seeks to obtain or communicates or seeks to communicate criminal offender record information in the furtherance of his or her official duties"). The Supreme Judicial Court has upheld the regulation authorizing agencies to disseminate CORI when "'specifically related to and contemporaneous with an investigation or prosecution'" as a "reasonable" interpretation of the statute under the agency's "broad delegation of rule making authority." *Bellin*, 435 Mass. at 265-66, 268.

If a person believes the CORI statute or regulations may have been violated, that person may file a complaint with the Criminal Record Review Board. 803 CMR 2.25 (authorizing complaints for violations of CORI statute or regulations and describing procedures); see also 803 CMR 7.12 (complaints specifically regarding wrongful agency attempts to obtain CORI from DCJIS). Among other powers, the Board may impose a civil fine of up to \$5,000 for each knowing violation and refer complaints to state and federal criminal justice agencies. 803 CMR 2.26(3)(1)-(m). That the Board has reportedly not yet received and adjudicated a complaint relating to a booking photograph or police report does not negate the availability of such remedies. *Cf. Globe Br.* 42 n.9.

Although the Superior Court below expressed concern that law enforcement agencies may be inconsistent in the extent to which they treat booking photographs and police reports as CORI-protected, see RA 91, the appropriate response to such a concern is not to obliterate CORI protections for arrest-related records for all persons in the Commonwealth.⁵ Rather, the appropriate response is to ensure that all CORI-holders follow the law set forth by the Legislature, as interpreted and implemented by DCJIS, and as further declared by the courts. Indeed, entry of the declaration urged by DCJIS - that booking photographs and arrest- and charge-related police reports are protected as CORI - will clarify for agencies across the Commonwealth what the CORI law protects.

⁵ In this regard, DCJIS and MSP note that the declaration entered below does not, on its face, declare one rule of law applicable to all persons within the Commonwealth. See RA 85. Rather, the Superior Court declared that the CORI law "does not prohibit the defendants from providing public access to (a) booking photographs of *police officers arrested for alleged crimes*; [or] police incident reports involving public officials[.]" *Id.* (emphasis added). The court presumably limited the declaration to tailor it to the facts presented. However, there is no basis in the CORI law for distinguishing between CORI subjects who are public officials or police officers, and CORI subjects who are members of the general public. Accordingly, any ruling of law of this Court would apply equally to all persons in the Commonwealth.

II. The CORI Law's Text and Its Recognized Purposes Refute the Globe's Contention That the 2010 Amendments Eliminated All CORI Protections Except for the Contents of DCJIS's Database.

The Globe's account of the 2010 amendments as eliminating all protections for CORI except CORI in the form of DCJIS's iCORI database is at odds with both the statute's text and its recognized purposes.

The Globe's interpretation is belied by the Legislature's leaving undisturbed many aspects of the statute evincing continued protection for all forms of CORI. Most importantly, the Legislature retained the broad definition of CORI as comprising records and information in "any" form held by any Massachusetts criminal justice agency, G.L. c. 6, § 167, while providing for regulated access to such information solely through the iCORI database, G.L. c. 6, § 172. Although the Globe criticizes DCJIS's defense of this "sweeping, blanket" protection, Br. 43, it is the Legislature itself that long ago enacted such broad protections - and then, in the 2010 amendments, provided considerably greater (albeit regulated) access to "official" CORI through DCJIS's database.

The Legislature also left intact numerous other aspects of the law demonstrating its continued intent to protect non-iCORI information, with respect to many of which provisions the Globe has not even attempted to reconcile its theory. For example, the provision making chronological booking logs public records, G.L.

c. 6, § 172(m), would be superfluous under the Globe's theory, because a booking log is a record created by a police department in the first instance, not received from DCJIS. The Globe's only response is to say that § 172(m) is a dead letter. Br. 39.⁶ See also, e.g., Comm. Br. 36-39 (discussing, *inter alia*, G.L. c. 6, §§ 167A(c), 171, 171A, 175, 178B); Globe Br. 6, 32-33 & n.3 (not mentioning these provisions at all, or simply noting their existence without argument).

And the Globe offers no response to the point that the recent criminal justice reform bill evinces the Legislature's continued understanding that police logs are police departments' only arrest-related records that are not CORI-protected. See Comm. Br. 50-51 (discussing G.L. c. 276, §§ 100E *et seq.*); Globe Br. 6 (not mentioning these provisions). That legislation created new expungement procedures to provide further privacy protections for arrestees, including for persons whose records do not include a conviction, and provides that all relevant "police

⁶ The Globe notes in passing that the Legislature's 2010 amendments deleted language in G.L. c. 6, § 172(m) limiting public access to *alphabetical indices* of police logs and chronologically maintained court records. Br. 35, n.5. The salience of these deletions seems limited, as the constraint on access to alphabetical indices of court records was struck down on First Amendment grounds 25 years ago. See *Globe Newspaper Co. v. Fenton*, 819 F. Supp. 89 (D. Mass. 1993).

logs" be expunged – but no other police records. See G.L. c. 276, §§ 100H, 100L(a). Thus, the Legislature evidently believed that, in order to create this new privacy protection for past arrests, only the public police logs needed to be expunged; arrest-related information held by agencies in any other form would be CORI-protected.

Moreover, the Globe's theory is fundamentally at odds with the Legislature's well established purposes in passing the 2010 amendments, acknowledged by the Globe itself: "to 'provid[e] an official avenue for criminal history information [and] to balance a recognized need for broader access to criminal history information with a desire to minimize reliance on inaccurate or unauthorized criminal history information sources." Globe Br. 33-34 n.33 (quoting *Commonwealth v. Pon*, 469 Mass. 296, 304-05 (2014)). Under the Globe's theory, rather than the statute channeling requestors to the "official avenue" presented by the DCJIS database, *Pon*, 469 Mass. at 304, requestors may go to any criminal justice agency and request arrest-related information or any other CORI possessed by that agency, in any form, so long as the requested information is not furnished directly from DCJIS's database. And rather than minimizing reliance on "inaccurate or unauthorized information," *id.* at 305, the Globe's interpretation would allow

rampant access to both: to inaccurate or misleadingly incomplete information (for example, regarding arrests that proved to be unfounded) and to unauthorized information (that is, information that might be accurate but to which a particular requestor would not be entitled through iCORI, for example regarding a sealed conviction or one eligible for sealing).

The Globe offers no convincing means of reconciling its construction with the Legislature's evident aims. The Globe seems to suggest that the Legislature chose to protect only the database, and nothing else, because only the database contains the full gamut of compiled information, "not found in paper files maintained by any individual law enforcement agencies." Br. 36. Notably, however, the Globe cites no legislative history whatsoever supporting this theory. See *id.* And, if allowed, such broad access to CORI could aid the proliferation of the very internet-based and potentially inaccurate sources of CORI information that the Legislature was seeking to displace by granting broader access to "official" CORI. See *Pon*, 469 Mass. at 304 ("This expansion of access to official CORI records reflects a recognition . . . that making official CORI records available more broadly would help steer employers and others away from reliance on potentially inaccurate sources of criminal history information made possible

by technological advances since the initial passage of the CORI act[.]").⁷

In sum, the statute rebuts any suggestion that the Legislature intended to strip CORI protections from all information except as compiled by DCJIS.

III. Booking Photographs and Police Reports Do Not Categorically Fall Within the CORI Exceptions Making Public Certain Otherwise-Protected Records.

Nor do the circumscribed exceptions to CORI protection in G.L. c. 6, § 172(m) remove CORI

⁷ Nor is there merit to the Globe's objection that DCJIS's interpretation means that the criminal penalties in G.L. c. 6, § 178 sweep overly broadly, potentially extending to prosecutions of the press for republishing CORI released by criminal justice agencies. Globe Br. 39-42. The provision the Globe highlights makes it a crime to "knowingly communicate[] or attempt[] to communicate [CORI] to any other individual or entity *except in accordance with the provisions of sections 168 through 175.*" G.L. c. 6, § 178 (emphasis added). Sections 168 through 175 do not purport to regulate the press, nor prohibit further dissemination by recipients of CORI except in connection with official requests to DCJIS itself. See generally G.L. c. 6, § 172; see, e.g., *id.* § 172(f) (providing that "[a] requestor shall not disseminate [CORI] except upon request by a subject"; that "[a] requestor shall maintain a secondary dissemination log . . . subject to audit by the department"; and that "a requestor shall not maintain a copy, electronic or otherwise, of requested [CORI] *obtained from the department* for more than 7 years" (emphasis added)). Accordingly, for reasons in part founded in the rule of lenity cited by the Globe, Br. 41, this criminal provision would not and should not apply where a newspaper republishes CORI released by an agency like a police department, because such republication is not barred by the statute.

protection from all booking photographs and arrest- and charge-related police reports.

As discussed in the opening brief, the CORI exception for public court files in § 172(m)(2) does not eliminate all such CORI protection. Comm. Br. 26-28. The Globe now tacitly admits that photographs and arrest-related reports may not even be in a public court file. See Globe Br. 47 (arguing only that these materials "routinely are filed," and that, "*so long as the case file is public*, the records are subject to mandatory disclosure" (emphasis added)). A reading of the court-file exception as applying to any record created by a criminal justice agency that *could potentially* end up in a court file would eliminate all or nearly all CORI protections. Certainly, the Supreme Judicial Court did not so interpret the exception in the *Middle District* case, where the court simply read the "court file" exception to apply not only to docket numbers within the courthouse, but also to copies thereof in parties' hands. See *Globe Newspaper Co. v. Dist. Att'y for the Middle Dist.*, 439 Mass. 374, 382 (2003) (court-file exception applied because "[d]ocket numbers are assigned chronologically and maintained by courts as part of their court records" and do "not cease to be a 'court' record when . . . distributed to the parties to a case"). Here, by contrast, the records are created by a police

department and are not inherently part of "chronologically maintained court records of public judicial proceedings." G.L. c. 6, § 172(m)(2).

Such records also do not fall within the exception in G.L. c. 6, § 172(m)(1) for "police daily logs, arrest registers, or other similar records compiled chronologically." The Globe briefly argues in the alternative for the first time on appeal that this exception may apply, because "booking photographs are 'similar records' that law enforcement agencies compile on a temporal basis prior to the commencement of criminal proceedings[.]" Br. 47-48.⁸ The form and contents of a police log are prescribed by statute: the log consists of a single record, to which entries are added over time in order. See G.L. c. 41, § 98F (requiring police departments to maintain "a daily log, written in a form that can be easily understood, recording, in chronological order, all responses to valid complaints received, crimes reported, the names,

⁸ Below, the Globe argued only that the court-records exception in § 172(m)(2) extended to booking photographs and arrest-related police reports, and did not additionally argue that the police-blotter exception in § 172(m)(1) extended to these materials. See RA 21, ¶ 76 (complaint's allegation regarding court-record exception, citing *Middle Dist.*, 439 Mass. at 383). Accordingly, the parties did not develop a factual record on this police-blotter issue, which the Globe has waived. See *Royal Indem. Co. v. Blakely*, 372 Mass. 86, 88 (1977) (waiver rule "has particular force where the other party may be prejudiced by the failure to raise the point below").

addresses of persons arrested and the charges against such persons arrested"). Although it is unclear precisely what the Globe means in asserting that booking photographs and police reports are similar merely because they are "compile[d] on a temporal basis" - indisputably, like many records, they do accumulate over time - the Globe makes no clear argument that a "log" or "register" similar to the form prescribed by G.L. c. 41, § 98F exists for booking photographs or police reports, see Br. 47-48, and the Legislature has not required such a log or register to be created by statute to ensure public access to such materials, see G.L. c. 41, § 98F (prescribing contents of required daily log). The exception for these records therefore does not apply.

CONCLUSION

For the foregoing reasons, this Court should vacate the judgment below and remand with instructions to order entry of a judgment in favor of defendants declaring that the requested records are exempt from disclosure under G.L. c. 4, § 7, cl. 26(a), because records containing arrest- or charge-related information regarding an identifiable individual, including in the form of a booking photograph or police report, are protected as CORI under G.L. c. 6, §§ 167, 172, and 178.

Respectfully submitted,

MAURA HEALEY
ATTORNEY GENERAL

/s Elizabeth N. Dewar
Elizabeth N. Dewar, BBO No. 680722
State Solicitor
Daniel J. Hammond, BBO No. 559475
Assistant Attorney General
One Ashburton Place, 20th Floor
Boston, MA 02108-1598
(617) 963-2204
bessie.dewar@mass.gov

*Counsel for Appellants Department
of Criminal Justice Information
Services and Massachusetts State
Police*

Date: December 7, 2018

CERTIFICATION PURSUANT TO MASS. R. APP. P. 16(K)

I, Elizabeth N. Dewar, certify that the foregoing
brief complies with all rules of court pertaining to
the filing of briefs, including, but not limited to,
Mass. R. App. P. 16, 18, and 20.

/s Elizabeth N. Dewar
Elizabeth N. Dewar
December 7, 2018

CERTIFICATE OF SERVICE

I, Elizabeth N. Dewar, hereby certify that I have this day served the foregoing brief through the Appeals Court's e-filing system on the following registered representatives:

Jonathan M. Albano, Esq.
Morgan, Lewis & Bockius LLP
One Federal Street
Boston, MA 02110
jonathan.albano@morganlewis.com

Catherine Lizotte, Esq.
Boston Police Department
Office of the Legal Advisor
1 Schroeder Plaza
Boston, MA 02120-2014
catherine.lizotte@boston.gov

/s Elizabeth N. Dewar
Elizabeth N. Dewar
December 7, 2018

ADDENDUM

803 CMR 7.00 *et seq.*.....29

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

803 CMR 7.00: CRIMINAL JUSTICE INFORMATION SYSTEM (CJIS)

Section

- 7.01: Purpose and Scope
- 7.02: Definitions
- 7.03: CJA Access to the CJIS
- 7.04: Background Check Requirements
- 7.05: Maintenance of Municipal and Regional Systems
- 7.06: CJIS User Agreement and Global Justice/Public Safety Information Sharing Policy
- 7.07: Roles and Responsibilities
- 7.08: Fingerprinting
- 7.09: Prohibited Access to the CJIS
- 7.10: Dissemination of CORI to a CJA
- 7.11: Logging Requirements for Information Dissemination
- 7.12: Access to Criminal History Information by Non-criminal Justice Agencies
- 7.13: Complaints Alleging Improper Access to, or Dissemination of, CJIS Information
- 7.14: Penalties for Improper Access to, or Dissemination of, CJIS Information
- 7.15: Severability

7.01: Purpose and Scope

- (1) 803 CMR 7.00 is issued in accordance with M.G.L. c. 6, §§ 167A and 172, and in accordance with 28 CFR 20 as it relates to criminal justice information systems maintained by the FBI.
- (2) 803 CMR 7.00 sets forth the roles, responsibilities, and policies that apply to all agencies and individuals either directly accessing the Criminal Justice Information System (CJIS) or using the data obtained from or through it.
- (3) 803 CMR 7.00 applies to all criminal justice agencies, as defined by both M.G.L. c. 6, § 167 and 28 CFR 20, and to all individuals accessing, using, collecting, storing, or disseminating criminal justice information, including criminal history record information, obtained from or through the CJIS or any other system or source to which the DCJIS provides access.
- (4) Nothing contained in 803 CMR 7.00 shall be interpreted to limit the authority granted to the Criminal Record Review Board (CRRB) or to the DCJIS by the Massachusetts General Laws.

7.02: Definitions

All definitions set forth in 803 CMR 2.00: *Criminal Offender Record Information (CORI)*, 5.00: *Criminal Offender Record Information (CORI) - Housing*, 8.00: *Obtaining Criminal Offender Record Information (CORI) for Research Purposes*, 9.00: *Victim Notification Registry (VNR)*, 10.00: *Gun Transaction Recording* and 11.00: *Consumer Reporting Agency (CRA)* are incorporated in 803 CMR 7.02 by reference. The following additional words and phrases as used in 803 CMR 7.00 shall have the following meanings:

Agency Head. The chief law enforcement or criminal justice official (*e.g.*, Chief of Police, Colonel, Commissioner, Executive Director, *etc.*) at an agency with access to the CJIS or the information contained therein.

Backup CJIS Representative. An employee of a criminal justice agency designated by the agency head to be the agency's secondary point of contact with the DCJIS.

Criminal History Record Information (CHRI). Criminal history record information means information collected nationwide by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, and release. Criminal History Record Information (CHRI) does not include identification information such as fingerprint records if such information does not indicate the individual's involvement with the criminal justice system.

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.02: continued

CJIS Authorized User. An employee within a criminal justice agency that is authorized to use the CJIS in performance of the employee's official duties.

Criminal Justice Agency (CJA). Pursuant to M.G.L. c. 6, § 167, criminal justice agencies are defined in Massachusetts as "those agencies at all levels of government which perform as their principal function, activities relating to:

- (a) crime prevention, including research or the sponsorship of research;
- (b) the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders; or
- (c) the collection, storage, dissemination, or usage of criminal offender record information".

The DCJIS is also required to adhere to the federal definition of a criminal justice agency found in 28 CFR 20 when granting access to data existing in systems and sources outside of the Commonwealth. 28 CFR 20 defines a criminal justice agency as courts and those governmental agencies or any sub-unit thereof that perform the administration of criminal justice pursuant to a statute or executive order, and that allocates a substantial part of its annual budget to the administration of criminal justice, including state and federal Inspector General Offices.

Criminal Justice Information System (CJIS). Local, state, regional, interstate, and federal information systems, including databases, computer applications, and data networks used by criminal justice and public safety agencies to enhance public safety, improve interagency communications, promote officer safety, and support quality justice and law enforcement decision making.

CJIS Representative. An employee of a criminal justice agency designated by the agency head to be the agency's primary point of contact with the DCJIS.

CJIS Systems Agency (CSA). The agency designated by the FBI to provide management control of FBI CJIS systems within a state. The DCJIS is the Massachusetts designee.

CJIS Systems Officer (CSO). The individual designated by the CSA within a state who maintains management oversight of FBI CJIS systems on behalf of the FBI. This is an employee of the DCJIS.

CJIS User Agreement. An agreement executed between the DCJIS and an authorized criminal justice agency that sets forth the rules and responsibilities for accessing and using information maintained within the CJIS or shared *via* the CJIS network. As referenced in 803 CMR 7.00, "Global Justice/Public Safety Information Sharing Policy" and "DCJIS Policy" shall be synonymous with CJIS User Agreement.

CJIS Technical Representative. An employee of a criminal justice agency designated by the agency head to serve as the technical liaison with the DCJIS.

FBI CJIS Security Policy (CSP). The FBI CJIS Division document that describes the security requirements to which all CJIS user agencies must adhere.

Offense-based Tracking Number (OBTN). A unique identifying number assigned by a law enforcement or criminal justice agency at the time of booking and associated with a fingerprint-supported criminal event.

Originating Agency Identifier (ORI). A unique identifier assigned by the FBI CJIS Division to each agency authorized to access or submit data to FBI CJIS information systems.

Public Safety Information System(s). All databases, applications, systems, or network services managed or provided by the DCJIS and used by law enforcement and justice officials for authorized criminal justice purposes.

7.03: CJA Access to CJIS

- (1) A CJA shall request CJIS access through the DCJIS.

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.03: continued

(2) A CJA seeking to gain access to local or Commonwealth criminal justice information systems shall meet the definition of a criminal justice agency as defined in M.G.L. c. 6, §§ 167 and 172(1)(a), and 803 CMR 7.02.

(3) CJAs seeking access to national criminal justice information systems shall also qualify under the federal definition found at 28 CFR 20. Only those agencies that meet the FBI requirements shall be provided with an ORI.

7.04: Background Check Requirements

(1) State, national, and state-of-residency fingerprint-based background checks shall be conducted on all individuals, including vendors and contractors, with unescorted access to secure areas of a law enforcement or criminal justice agency as required by the CSP. These checks are also required for individuals who have direct access to the CJIS system or to local systems and networks which connect to the CJIS network, such as dispatchers and city/town information technology staff, whether or not they have unescorted access to secure areas.

7.05: Maintenance of Municipal and Regional Systems

Municipal and regional information systems and networks used to access the CJIS or connected to the CJIS network shall comply with the standards identified within the latest version of the CSP.

7.06: CJIS User Agreement and Global Justice/Public Safety Information Sharing Policy

The DCJIS Policy shall be executed annually by each agency with direct access to the CJIS or to the information contained within, or obtained through, the CJIS. In addition, an agency shall execute a new DCJIS Policy with the DCJIS whenever there are changes to the agency head, the CJIS representative, the backup CJIS representative, or the CJIS technical representative.

7.07: Roles and Responsibilities

(1) The DCJIS is the FBI CSA for Massachusetts. In this capacity, the DCJIS shall be responsible for the administration and management of the FBI CJIS on behalf of the FBI, and shall be responsible for overseeing access to all FBI systems and information by Massachusetts agencies, as well as for ensuring system security, training, policy compliance, and auditing.

(2) Each agency head shall be responsible for:

- (a) designating a CJIS representative, a backup CJIS representative, and a technical representative; the CJIS representative or backup CJIS representative may also serve as the technical representative if necessary;
- (b) ensuring that all agency users of the CJIS, or the information obtained from it, have been trained, tested, and certified within six months of hire and biennially thereafter;
- (c) responding to audit questionnaires, complaints, and any other inquiries from the DCJIS or from the FBI within the time period allowed;
- (d) providing the results of any investigation into the misuse of the CJIS or any other system or source to which the DCJIS provides access;
- (e) reporting any misuse of the CJIS, including improper access to, or improper dissemination of, information, as soon as possible to the DCJIS;
- (f) executing the DCJIS Policy as required;
- (g) ensuring that the agency adheres to all CJIS and FBI policies and procedures, including the FBI CJIS Security Policy;
- (h) notifying the DCJIS as soon as practicable of any changes in contact information for the agency, the agency head, the CJIS representative, the backup CJIS representative, and the technical representative; and
- (i) ensuring compliance with all state and federal laws, regulations, and policies related to the CJIS and any other system or source to which the DCJIS provides access.

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.07: continued

- (3) The CJIS representative and the backup CJIS representative shall be responsible for:
 - (a) training, testing, and certifying agency users within six months of hire and biennially thereafter;
 - (b) responding to audit questionnaires, complaints, and/or any other inquiries from the DCJIS or from the FBI within the time period allowed, as well as for providing the results of any investigations into the misuse of the CJIS and any other system or source to which the DCJIS provides access;
 - (c) reporting any misuse of the CJIS, including improper access to, or improper dissemination of, information, as soon as possible to the DCJIS;
 - (d) executing the DCJIS Policy as required;
 - (e) ensuring that the agency adheres to all CJIS and FBI policies and procedures;
 - (f) notifying the DCJIS as soon as practicable of any changes in contact information for the agency, the agency head, the CJIS Representative, the backup CJIS Representative, and the technical representative; and
 - (g) ensuring compliance with all state and federal laws, regulations, and policies related to the CJIS and any other system or source to which the DCJIS provides access.
- (4) The CJIS technical representative shall be responsible for:
 - (a) maintaining and coordinating the agency's technical access to public safety information systems;
 - (b) maintaining CJIS system security requirements;
 - (c) reporting any misuse of the CJIS, including improper access to, or improper dissemination of, information, as soon as possible to a supervisor or commanding officer; and
 - (d) complying with all state and federal laws, regulations, and policies related to the CJIS.
- (5) A CJIS authorized user shall be responsible for:
 - (a) use of the CJIS for authorized and official criminal justice purposes only;
 - (b) successfully completing all required training;
 - (c) reporting any misuse of the CJIS, including improper access to, or improper dissemination of, information, as soon as possible to a supervisor or commanding officer; and
 - (d) complying with all state and federal laws, regulations, and policies related to the CJIS and to the use of computers.
- (6) CJIS certification training shall be completed every two years. In addition, authorized users may be required to complete additional training for specific applications and information systems. 803 CMR 7.07(6) shall apply to any individual who either uses the CJIS directly or who uses information obtained from the CJIS or from any other system or source to which the DCJIS provides access.
- (7) The CJIS shall be accessed only by trained and certified criminal justice officials for authorized criminal justice and law enforcement purposes.

7.08: Fingerprinting

- (1) Fingerprints shall be submitted to the Massachusetts State Police SIS for criminal justice purposes in the following instances:
 - (a) criminal justice employment background checks;
 - (b) felony arrests by law enforcement agencies pursuant to M.G.L. c. 263, § 1;
 - (c) all arrests for felony violations of M.G.L. c. 94C pursuant to M.G.L. c. 94C, § 45;
 - (d) detentions and incarcerations by the Department of Correction and Sheriffs' Departments (Jails and Houses of Correction); and
 - (e) licensee screening for specific categories as authorized by ordinance, bylaw, state statute, or federal law and which have been approved by the FBI.
- (2) Fingerprints may also be submitted to the SIS for misdemeanor arrests.
- (3) CJAs submitting fingerprints shall comply with DCJIS, Massachusetts State Police, and FBI policies and requirements for the specific type of fingerprint submission.

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.08: continued

- (4) All fingerprint submissions shall include an agency-assigned OBTN formatted in the manner prescribed by the SIS.

7.09: Prohibited Access to the CJIS

- (1) The CJIS shall not be accessed for any non-criminal justice purpose. The only non-criminal justice purpose for which a user may access the CJIS is training. When using the CJIS for training purposes, users shall use the test records provided by the DCJIS. Users shall not run test records or train with their own personal information or with the personal information of another real individual.
- (2) The CJIS shall only be accessed for authorized criminal justice purposes, including:
- (a) criminal investigations, including motor vehicle and driver's checks;
 - (b) criminal justice employment;
 - (c) arrests or custodial purposes;
 - (d) civilian employment or licensing purposes as authorized by law and approved by the FBI; and
 - (e) research conducted by the CJA.

7.10: Dissemination of CORI to a CJA

- (1) CORI may be provided to another criminal justice agency for official criminal justice purposes.
- (2) A CJA with official responsibility for a pending criminal investigation or prosecution may disseminate CORI that is specifically related to, and contemporaneous with, an investigation or prosecution.
- (3) A CJA may disseminate CORI that is specifically related to, and contemporaneous with, the search for, or apprehension of, any person, or with a disturbance at a penal institution.
- (4) A CJA may disseminate to principals or headmasters CORI relating to a student 18 years of age or older charged with, or convicted of, a felony offense, provided that the information provided to school officials is limited to the felony offense(s) that may subject the student to suspension or expulsion pursuant to the provisions of M.G.L. c.71, § 37H½.
- (5) A CJA may disclose CORI for the purpose of publishing information in the department's daily log as required by M.G.L. c. 41, § 98F.
- (6) A CJA may disseminate CORI as otherwise authorized by law in the interest of public safety.
- (7) Pursuant to M.G.L. c. 6, § 175, a CJA may disseminate CORI to the individual to whom it pertains, or to the individual's attorney with a signed release from the individual. The CORI provided shall be limited to information compiled by the CJA, such as a police report prepared by the CJA. A CJA may not provide an individual with any CORI obtained through the CJIS.
- (8) If an individual seeks to access the individual's national criminal history, the individual shall contact the FBI. Likewise, requests for driver history information shall be submitted to the Massachusetts Registry of Motor Vehicles. All other information contained in the CJIS shall only be disseminated to other criminal justice agencies for official criminal justice purposes.
- (9) Any requests for an individual's statewide CORI shall be directed to the DCJIS.

7.11: Logging Requirements for Information Dissemination

- (1) A CJA that provides information obtained from or through the CJIS, including CORI and criminal history record information, to another authorized CJA (or to an individual employed by an authorized CJA) other than the inquiring CJA, shall maintain a secondary dissemination log. The log shall contain the following:

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.11: continued

- (a) subject name;
 - (b) subject date of birth;
 - (c) date and time of the dissemination;
 - (d) name of the individual to whom the information was provided;
 - (e) name of the agency for which the requestor works; and
 - (f) specific reason for the dissemination.
- (2) The name and address of a motor vehicle owner may be provided to a tow company only if the tow company has a contract directly with the CJA; the contract cannot be with the city or town.
- (a) A CJA shall make an entry into a secondary dissemination log each time it releases information to a tow company.
 - (b) In addition to the information identified 803 CMR 7.11(1), the CJA shall record the registration number and the registration state, or the vehicle identification number, of the towed vehicle in the secondary dissemination log.

7.12: Access to Criminal History Record Information by Non-criminal Justice Agencies

- (1) The DCJIS may grant non-criminal justice agencies access to Criminal History Record Information (CHRI) in accordance with state and federal laws and regulations.
- (2) In order to access CHRI in accordance with applicable law, the non-criminal justice agency head shall be responsible for the following:
- (a) executing a Non-criminal Justice Agency User Agreement with the DCJIS;
 - (b) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;
 - (c) executing and providing the DCJIS with an employee designation form for each employee with direct access to the DCJIS system used to obtain CHRI;
 - (d) ensuring that all employees with direct access to the DCJIS system used to obtain CHRI have been fingerprinted and have had a complete background investigation in accordance with the latest version of the CSP;
 - (e) designating a local agency security officer (LASO);
 - (f) ensuring that all employees with access to CHRI have completed an Individual Agreement of Non-disclosure (AOND) form;
 - (g) ensuring that all employees with access to CHRI have completed training;
 - (h) responding to audit questionnaires, complaints, and any other inquiries from the DCJIS or from the FBI within the time period allowed;
 - (i) reporting any misuse of CHRI, including improper access to, or improper dissemination of, CHRI, as soon as possible to the DCJIS;
 - (j) providing the results of any investigation into the misuse of CHRI or any system or source to which the DCJIS provides access;
 - (k) ensuring that the agency adheres to all DCJIS and FBI policies and procedures, including the CSP;
 - (l) notifying the DCJIS as soon as practicable of any changes in contact information for the agency, including the agency head, local agency security officer, and any employees authorized to access DCJIS systems;
 - (m) ensuring compliance with all state and federal laws, regulations, and policies related to CHRI, the CJIS, and any other system or source to which the DCJIS provides access.
- (3) The local agency security officer shall be responsible for the following:
- (a) completing the fingerprint-based criminal history background investigation, training, and AOND form;
 - (b) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;
 - (c) ensuring compliance with security procedures related to CHRI and DCJIS systems;
 - (d) coordinating and reporting all personnel security clearance requests and any subsequent criminal history activity relating to an approved employee to the DCJIS CJIS Systems Officer (DCJIS CSO) within five business day.
 - (e) notifying the DCJIS Information Security Officer (ISO) of any and all security incidents within 48 hours of the discovery of the incident.

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.12: continued

- (f) responding to audit questionnaires, complaints, and any other inquiries from the DCJIS or from the FBI within the time period allowed;
 - (g) reporting any misuse of CHRI, including improper access to, or improper dissemination of, CHRI, as soon as possible to the DCJIS;
 - (h) providing the results of any investigations into the misuse of CHRI or any system or source to which the DCJIS provides access;
 - (i) ensuring that the agency adheres to all DCJIS and FBI policies and procedures, including the CSP;
 - (j) notifying the DCJIS as soon as practicable of any changes in contact information for the agency, including the agency head, local agency security officer, and any employees authorized to access DCJIS systems;
 - (k) keeping user codes and passwords used to access CHRI confidential; and
 - (l) ensuring compliance with all state and federal laws, regulations, and policies related to CHRI, the CJIS, and any other system or source to which the DCJIS provides access.
- (4) Employees designated by their agency head to access CHRI shall be responsible for the following:
- (a) completing the finger print-based criminal background investigation (employees with direct access to DCJIS systems and CHRI only);
 - (b) completing the Individual AOND and training requirements;
 - (c) submitting requests for, reviewing, and disseminating CHRI results only as authorized by law;
 - (d) reporting any subsequent criminal activity to the local agency security officer within five days;
 - (e) keeping user codes and passwords used to access CHRI confidential;
 - (f) notifying the DCJIS as soon as practicable of any changes in contact information; and
 - (g) ensuring compliance with all state and federal laws, regulations, and policies related to CHRI, the CJIS, and any other system or source to which the DCJIS provides access.
- (5) CHRI shall not be disseminated except in accordance with the law that provides the non-criminal justice agency with access to CHRI. In the event CHRI is disseminated, the non-criminal justice agency shall maintain a secondary dissemination log. The log will record the following information:
- (a) the subject's name;
 - (b) the subject's date of birth;
 - (c) the date and time of dissemination;
 - (d) the name of the person to whom the CHRI was disseminated along with the name of the organization for which the person works; and
 - (e) the specific reason for dissemination.
- (6) Each entry in the secondary dissemination log will be maintained for a minimum of one year.
- (7) Non-criminal justice agencies that are inclined to deny an individual on the basis of his or her CHRI must first provide the individual with information on how to change, correct or update his or her criminal records in accordance with 28 CFR 16.34.
- (8) Paper copies of CHRI shall be stored in locked file cabinets and shall not be left unattended.
- (9) Electronic copies of CHRI shall be stored in accordance with the provisions of the latest version of the CSP.
- (10) CHRI shall only be disposed of in a secure manner. Physical media must be cross-shredded and/or burned, and electronic records must be deleted and repeatedly over-written with random 0s and 1s, or the media must be degaussed.

7.13: Complaints Alleging Improper Access to, or Dissemination of, CJIS Information

An individual may file a complaint with the DCJIS upon the belief that an agency improperly obtained, or attempted to obtain, CJIS information regarding the individual.

803 CMR: DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES

7.13: continued

- (a) The DCJIS shall review the complaint. If it contains a sufficient statement describing the allegation, DCJIS staff shall conduct an audit of the CJIS system to determine if a specific CJA or authorized CJIS user accessed the individual's information through the CJIS during the time period specified in the complaint. If the audit confirms such access, then DCJIS staff may contact the agency head to request an internal investigation.
- (b) If requested by the DCJIS, the agency head shall conduct an investigation into the alleged misuse according to the rules, regulations, and policies in place at the agency. At the conclusion of the investigation, the agency head shall provide the DCJIS with a written summary of the investigation's findings. In addition, if the agency head substantiates the allegation(s), the written summary shall provide details of the specific actions taken to correct the misuse as well as details of the sanctions imposed on the subject(s) of the investigation, if any.
- (c) The DCJIS may impose additional penalties as outlined in CJIS policy and 803 CMR 7.00.

7.14: Penalties for Improper Access to, or Dissemination of, CJIS Information

- (1) An individual found in violation of 803 CMR 7.00, or of DCJIS or FBI policies and procedures, may be subject to federal and state civil and criminal penalties for improper access to, or dissemination of, information obtained from or through the CJIS pursuant to M.G.L. c. 6, §§ 167A(d), 168 and 178, and 28 CFR 20.
- (2) Such civil sanctions and penalties may include, but not be limited to, fines issued by the Commissioner of the DCJIS pursuant to M.G.L. c. 6, § 167A(d),

7.15: Severability

If any provision of 803 CMR 7.00, or the application thereof, is held to be invalid, such invalidity shall not affect the other provisions or the application of any other part of 803 CMR 7.00 not specifically held invalid and, to this end, the provisions of 803 CMR 7.00 and various applications thereof are declared to be severable.

REGULATORY AUTHORITY

803 CMR 7.00: M.G.L. c. 6, § 167A, c. 6, § 172, and 28 CFR 20: *Criminal Justice Information Systems.*